BEST AVAILABLE COPY

Please amend the claims to read:

1. (currently amended) In a data processing operation having
stored data in a plurality of data files, a system for
protecting said data files from unauthorized users compris-
ing:
    means for storing for each of said plurality of data
files, a backup file inaccessible to user requests;
    means for receiving user requests for access to data
files;
    means for determining whether said requests are unau-
thorized intrusions into said requested data files; and
    means responsive to an initial determination that a
request is unauthorized for destroying the requested data
files; and
    means for reloading a backup file for each destroyed
file.

2 and 3 (cancelled)

4. (original) The data processing operation system of claim
1 wherein said means for determining whether said user
requests are unauthorized intrusions include:
    means for determining whether a user access identifica-
tion code has been denied; and
    means for determining whether the user has copied the
requested files.

AUS920000935US1   2

1 5. (currently amended) In a communication network with
2 access to a plurality of network sites each having stored
3 data in a plurality of data files accessible in response to
4 requests from users at other sites in the network, a system
5 for protecting said network site data files from unautho-
6 rized users comprising:
7 means for storing for each of said plurality of data
8 files at said network site, a backup file inaccessible to
9 user requests;
10 means associated with a network site for
11 receiving user requests for access to data files;
12 means at said network site for determining whether said
13 user requests are unauthorized intrusions into said request-
14 ed data files; and
15 means at said network site responsive to an initial
16 determination that a request is unauthorized for destroying
17 the requested data files; and
18 means for reloading a backup file for each destroyed
19 file.

6 (cancelled)

AUS920000935US1   3

PATENT
09/801,614

1   7. (currently amended) In a World Wide Web communication
2   network with access to a plurality of open Web sites each
3   having stored data in a plurality of data files accessible
4   in response to requests from users at stations throughout
5   the Web, a system for protecting said open Web site data
6   files from unauthorized users comprising:
7   means for storing for each of said plurality of data
8   files at said open Web site, a backup file inaccessible to
9   user requests;
10   means associated with an open Web site for
11   receiving user requests for access to data files;
12   means at said open Web site for determining whether
13   said user requests are unauthorized intrusions into said
14   requested data files; and
15   means at said open Web site responsive to an initial
16   determination that a request is unauthorized for destroying
17   the requested data files; and
18   means for reloading a backup file for each destroyed
19   file.

8 and 9 (cancelled).

AUS920000935US1   4

1   10. (currently amended) In a data processing operation
2   having stored data in a plurality of data files, a method
3   for protecting said data files from unauthorized users
4   comprising:
5   storing for each of said plurality of data files, a
6   backup file inaccessible to user requests;
7   receiving user requests for access to data files;
8   determining whether said requests are unauthorized
9   intrusions into said requested data files; and
10   destroying the requested data files responsive to an
11 initial determination that a request is unauthorized; and
12   reloading a backup file for each destroyed file.

    11 and 12 (cancelled)

1   13. (original) The data processing method of claim 10 where-
2   in said step of determining whether said user requests are
3   unauthorized intrusions includes:
4   determining whether a user access identification code
5   has been denied; and
6   determining whether the user has copied the requested
7   files.

AUS920000935US1   5

PATENT
09/801,614

1   14. (currently amended)0 In a communication network with
2   access to a plurality of network sites each having stored
3   data in a plurality of data files accessible in response to
4   requests from users at other sites in the network, a method
5   for protecting said network site data files from
6   unauthorized users comprising:
7   storing for each of said plurality of data files at
8   said network site, a backup file inaccessible to user re-
9   quests;
10   receiving user requests for access to data files at a
11 network site;
12   determining at said network site whether said user
13 requests are unauthorized intrusions into said requested
14 data files; and
15   destroying the requested data files responsive to an
16 initial determination that a request is unauthorized; and
17   reloading a backup file for each destroyed file.

15 and 16 (cancelled)

AUS920000935US1   6

PATENT
09/801.614

1 17. (currently amended) In a World Wide Web communication
2 network with access to a plurality of open Web sites each
3 having stored data in a plurality of data files accessible
4 in response to requests from users at stations throughout
5 the Web, a method for protecting said open Web site data
6 files from unauthorized users comprising:
7   storing for each of said plurality of data files at
8 said open Web site, a backup file inaccessible to user
9 requests:
10   receiving user requests for access to data files at
11 said open Web site;
12   determining whether said user requests are unauthorized
13 intrusions into said requested data files at said open Web
14 site; ~~and~~
15   destroying the requested data files at said open Web
16 site responsive to an initial determination that a request
17 is unauthorized; and
18   reloading a backup file for each destroyed file.

18 and 19 (cancelled)

1 20. (original) The World Wide Web communication network
2 method of claim 17 wherein said step of determining whether
3 said user requests are unauthorized intrusions includes:
4   determining whether a user access identification code
5 has been denied; and
6   determining whether the user has copied the requested
7 files.

AUS920000935US1   7

PATENT
09/801,614

1   21. (currently amended) A computer program having code
2   recorded on a computer readable medium for protecting data
3   files from unauthorized users in a data processing operation,
4   having stored data in a plurality of data files, said
5   program comprising:
6   means for storing for each of said plurality of data
7   files, a backup file inaccessible to user requests:
8   means for receiving user requests for access to data
9   files;
10   means for determining whether said requests are unau-
11 thorized intrusions into said requested data files; and
12   means responsive to an initial determination that a
13 request is unauthorized for destroying the requested data
14 files; and
15   means for reloading a backup file for each destroyed
16 file.

    22 and 23 (cancelled)

1   24. (original) The computer program of claim 21 wherein said
2   means for determining whether said user requests are
3   unauthorized intrusions include:
4   means for determining whether a user access identifica-
5   tion code has been denied; and
6   means for determining whether the user has copied the
7   requested files.

AUS920000935US1   8

PATENT
09/801,614

1   25. (currently amended) A computer program having code
2   recorded on a computer readable medium for protecting data
3   files from unauthorized users in a communication network
4   with access to a plurality of network sites each having
5   stored data in a plurality of data files accessible in
6   response to requests from users at other sites in the
7   network, said program comprising:
8   means for storing for each of said plurality of data
9   files at said network site, a backup file inaccessible to
10 user requests;
11   means associated with a network site for
12 receiving user requests for access to data files;
13   means at said network site for determining whether said
14 user requests are unauthorized intrusions into said request-
15 ed data files; and
16   means at said network site responsive to an initial
17 determination that a request is unauthorized for destroying
18 the requested data files; and
19   means for reloading a backup file for each destroyed
20 file.

26 (cancelled)

AUS920000935US1   9

1   27. (currently amended) A computer program having code
2   recorded on a computer readable medium for protecting open
3   Web sites in a World Wide Web communication network with
4   access to a plurality of open Web sites each having stored
5   data in a plurality of data files accessible in response to
6   requests from users at stations throughout the Web, said
7   program comprising:
8   <u>means for storing for each of said plurality of data</u>
9   <u>files at said open Web site, a backup file inaccessible to</u>
10   <u>user requests;</u>
11   means associated with an open Web site for
12   receiving user requests for access to data files;
13   means at said open Web site for determining whether
14   said user requests are unauthorized intrusions into said
15   requested data files; ~~and~~
16   means at said open Web site responsive to a<u>n initial</u>
17   determination that a request is unauthorized for destroying
18   the requested data files; <u>and</u>
19   <u>means for reloading a backup file for each destroyed</u>
20   <u>file</u>.

  28 and 29 (cancelled)

1   30. (original) The computer program of claim 27 wherein said
2   means for determining whether said user requests are
3   unauthorized include:
4   means for determining whether a user access identifica-
5   tion code has been denied; and
6   means for determining whether the user has copied the
7   requested files.